User IDs and Passwords

ITS

IT Policies, Standards and Guidelines Home
Definitions
Violations

User Ids and passwords are an important aspect of information and information technology security. Employee logins are requested by Human Resources at the time of hire and are terminated when Human Resources notifies ITS the person is no longer employed. Accounts will not be created without Human Resources requesting them.

All users, whether internal, external, or temporary, and their activity on all IT systems should have User Ids that:

- are uniquely identifiable
- are enabled through appropriate authentication mechanisms
- are assigned access rights to all systems and data in line with defined and documented business needs and job requirements
- are only requested by user management, approved by system owners, and implemented by the appropriate local security administrator.

System Owners are responsible for maintaining user identification and access rights in a centrally managed repository.

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to information systems, services and applications unless specifically designated as a public access resource. All users (students, employees, contractors, and vendorsshall take the appropriate steps to select and secure their passwords. Failure to use a strong password or using a poorly chosen password when accessing information assets may result in the compromise of those assets.

This standard is designed to comply with applicable laws and regulations. However, if there is a conflict, applicable laws and regulations will take precedence.

Secure your device	All devices permanently or intermittently connected to CSU networks must have password access controls • Require a login to the device and make sure no one can bypass the login and access the device • Employ a no-activity screen saver that requires a password to reopen the screen • Lock the device screen before leaving the device unattended
Secure your data	Restrict access based on the need-to-know; privileges must not be extended unless a legitimate business-oriented need for such privileges exists • User-IDs and passwords for multi-user systems must be unique for each user • Each person accessing a resource should have their own User-ID and password on that resource. • Use of group passwords is prohibited - passwords and User-IDs s used by more than one person for example 5 people logging into Banner using the same User-ID and password. • System Administrator or superuser privileges should only be extended to those persons who have the primary responsibility for that system • Temporary or “first use” passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system, and have a limited life of inactivity before being disabled • To prevent “password guessing” attacks the number of consecutive attempts to enter an incorrect password must be strictly limited. If dial-up or other external network

Secure your device	All devices permanently or intermittently connected to CSU networks must have password access controls • Require a login to the device and make sure no one can bypass the login and access the device • Employ a no-activity screen saver that requires a password to reopen the screen • Lock the device screen before leaving the device unattended
	connections are involved, the session must be disconnected after the unsuccessful attempts

Secure your Password	All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators and/or helpdesk personnel or other members of ITS
	
	• If a user needs help and a support person needs to login as that user, the password should be reset by ITS and then reset for the user once support is done
	• In many cases, log files are maintained and you are responsible for activity by your user account
	• All user-level passwords shall be changed every one hundred and eighty (180) days.
	• Passwords shall not be stored in clear text and protected from viewing:
	  ○ Users shall not write passwords down or store them anywhere in their office or publically.
	  ○ The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Secure your device	All devices permanently or intermittently connected to CSU networks must have password access controls • Require a login to the device and make sure no one can bypass the login and access the device • Employ a no-activity screen saver that requires a password to reopen the screen • Lock the device screen before leaving the device unattended
	○ Written passwords will not be stored in the proximity of the device • Passwords shall not store in a file on any computer system, including smart devices unless encrypted • Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted
Select Strong Passwords	Strong passwords shall be constructed with the following characteristics: • Be at least ten characters in length • Must contain characters from at least two of the following four types of characters: • English upper case (A-Z) • English lower case (a-z) • Numbers (0-9) • Non-alphanumeric special characters ($, !, %, ^, …) • Must not contain the user's name or part of the user's name

Secure your device	All devices permanently or intermittently connected to CSU networks must have password access controls • Require a login to the device and make sure no one can bypass the login and access the device • Employ a no-activity screen saver that requires a password to reopen the screen • Lock the device screen before leaving the device unattended
	• Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.
Secure from external access	• All vendor-supplied default passwords must be changed before any computer or communications system is used for CSU business. This policy applies to passwords associated with end-user user-IDs, as well as passwords associated with systems administrator and other privileged user-IDs. • User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user. • Non-CSU employees will not be given network logins. • If you are using a contractor for web development, they will not be able to place the files on the web server. They must submit the files to the CSU user (floppy, e-mail, CD-ROM, etc...) and then the CSU user can place the files on the web server. • All system-level administrative passwords shall be changed every ninety (90) days. • If an account or password is suspected of being compromised, the incident must be reported to the

Secure your device	All devices permanently or intermittently connected to CSU networks must have password access controls • Require a login to the device and make sure no one can bypass the login and access the device • Employ a no-activity screen saver that requires a password to reopen the screen • Lock the device screen before leaving the device unattended
	appropriate authorities in accordance with local incident response procedures. • Password history must be enabled and configured to disallow usage of the same password for a set length of change cycles greater than four (4) times. Users and administrators must not be allowed to use the same password that has been used in the past four (4) changes. Users and administrators who have changed their user password or system password must not be allowed to change passwords immediately. This will prevent users and administrators from changing their passwords several times to get back to their old passwords.